CLAIMS

What is claimed is:

1. An apparatus for controlling access to a data security device within a data processing system, said apparatus comprising:

a persistent enable flag for providing control access to said data security device, wherein said persistent enable flag is write-accessible only in response to a detected power-on reset of said data processing system; and

a pending state change flag accessible by runtime program instructions, for setting an intended next state of said persistent enable flag such that control access to said data security device is enabled only during a subsequent power-on reset of said data processing system.

2. The apparatus of claim 1, further comprising:

a switched power input to said data security device;

a power-on reset detection latch for detecting the occurrence of power applied by said switched power input; and

means for determining the state of said power-on reset detection latch.

3. The apparatus of claim 2, further comprising means responsive to determining a set state of said power-on reset detection latch for:

determining the state of said pending state change flag; and

determining a next state of said persistent enable flag in accordance with the determined state of said pending state change flag.

4. The apparatus of claim 1, wherein said pending state change flag is write-accessible by said runtime program instructions and said persistent enable flag is read-only accessible to said runtime program instructions.

5. The apparatus of claim 1, wherein said persistent enable flag and said pending state change flag are non-volatile storage devices.

6. The apparatus of claim 1, wherein said data security device includes memory for receiving and storing data.

7. The apparatus of claim 1, wherein said data security device includes security portal functionality for controlling access to data stored within said data processing system.

8. The apparatus of claim 1, wherein said data security device includes control access includes functionality for enabling or disabling ownership of said data security device, enabling or disabling enablement of said data security device, or enabling or disabling activation of said data security device.

9. A method for providing secure controllability of a data security device within a data processing system, said method comprising:

responsive to a power-on reset cycle initiated within said data processing system:

determining the state of a pending state change flag, wherein said pending state change flag is accessible by runtime program instructions for setting an intended next state of a persistent enable flag that enables or disables runtime control access to said data security device; and

setting or resetting said persistent enable flag in accordance with the state of said pending state change flag.

10. The method of claim 9, wherein said power-on reset steps are preceded by the step of setting said pending state change flag in accordance with user input during runtime operations of said data processing system.

11. The method of claim 9, further comprising, responsive to said pending state change flag being set, setting said persistent enable flag such that control access for said data security device is enabled following said power-on reset.

12. The method of claim 9, further comprising, responsive to said pending state change flag being reset, resetting said persistent enable flag such that control access for said data security device is disabled following said power-on reset.

13. The method of claim 9, wherein said pending state change flag is write-accessible by said runtime program instructions and said persistent enable flag is read-only accessible to said runtime program instructions.

14. The method of claim 9, wherein said power-on reset cycle includes execution of startup program instructions, said method further comprising:

responsive to receiving user input within said data processing system, setting or resetting a state of said pending state change flag in accordance with said user input; and

only in response to execution of said startup program instructions within said non-volatile programmable memory unit, updating said persistent enable flag to said intended state in accordance with the state of said pending state change flag.

15. The method of claim 9, wherein said data security device includes memory for receiving and storing data.

16. The method of claim 9, wherein said data security device includes security portal functionality for controlling access to data stored within said data processing system.

17. The method of claim 9, wherein said data security device includes control access includes functionality for enabling or disabling ownership of said data security device, enabling or disabling enablement of said data security device, or enabling or disabling activation of said data security device.

18. A computer program product for providing secure controllability of a data security device within a data processing system, said program product comprising:

program instructions responsive to a power-on reset cycle initiated within said data processing system for:

determining the state of a pending state change flag, wherein said pending state change flag is accessible by runtime program instructions for setting an intended next state of a persistent enable flag that enables or disables runtime control access to said data security device; and

setting or resetting said persistent enable flag in accordance with the state of said pending state change flag.

19. The computer program product of claim 18, further comprising program instructions for setting said pending state change flag in accordance with user input during runtime operations of said data processing system.

20. The computer program product of claim 18, further comprising, program instructions responsive to said pending state change flag being set, for setting said persistent enable flag such that control access for said data security device is enabled following said power-on reset.

21. The computer program product of claim 18, further comprising, program instructions responsive to said pending state change flag being reset, for resetting said persistent enable flag such that control access for said data security device is disabled following said power-on reset.

22. The computer program product of claim 18, wherein said pending state change flag is write-accessible by said runtime program instructions and said persistent enable flag is read-only accessible to said runtime program instructions.

23. The computer program product of claim 18, wherein said power-on reset cycle includes execution of startup program instructions, said program product further comprising:

program instructions responsive to receiving user input within said data processing system, for setting or resetting a state of said pending state change flag in accordance with said user input; and

program instructions responsive only to execution of said startup program instructions within said non-volatile programmable memory unit, for updating said persistent enable flag to said intended state in accordance with the state of said pending state change flag.

24. The computer program product of claim 18, wherein said data security device includes memory for receiving and storing data.

25. The computer program product of claim 18, wherein said data security device includes security portal functionality for controlling access to data stored within said data processing system.

26. The computer program product of claim 18, wherein said data security device includes control access includes functionality for enabling or disabling ownership of said data security device, enabling or disabling enablement of said data security device, or enabling or disabling activation of said data security device.